

IN THE CLAIMS

The following is a complete listing of the claims, and replaces all earlier versions and listings.

1. (Previously Presented) A method of inserting a message into digital data representative of physical quantities, the message including ordered symbols, said method comprising the steps of:

segmenting the data into regions; and

associating at least one region with each symbol to be inserted, wherein, for each region into which a symbol in question is to be inserted, said method includes the steps of:

determining a pseudo-random function, from a key which depends on an initial key and on a length of the message,

modulating the symbol in question by the previously determined pseudo-random function in order to supply a pseudo-random sequence, and

adding the pseudo-random sequence to the region in question,

wherein the dependence of the key on the length of the message is provided by a dependence of the key on:

the number of times the symbol to be inserted has already been inserted into other regions, and

the ranking of the symbol among the ordered symbols.

2. (Canceled)

3. (Previously Presented) A method according to Claim 1, further comprising the step of transforming the digital data by a reversible transformation.

4. - 7. (Canceled)

8. (Previously Presented) A device for inserting a message into digital data representative of physical quantities, the message including ordered symbols, said device comprising:

means for segmenting the data into regions; and

means for associating at least one region with each symbol to be inserted,

wherein said device further includes:

means for determining a pseudo-random function, for each region into which a symbol in question is to be inserted, from a key which depends on an initial key and on a length of the message,

means for modulating the symbol in question by the previously determined pseudo-random function in order to supply a pseudo-random sequence, and

means for adding the pseudo-random sequence to the region in question,

wherein said means for determining a pseudo-random function is configured in such a way that a dependence of the key on the length of the message is provided by a dependence of the key on:

the number of times the symbol to be inserted has already been inserted into other regions, and

the ranking of the symbol among the ordered symbols.

9. (Canceled)

10. (Previously Presented) A device according to Claim 8, further comprising means for prior transformation of the digital data by a reversible transformation.

11. - 14. (Canceled)

15. (Previously Presented) A device according to Claim 8, wherein said steps of segmenting and associating, and the steps of determining, modulating, and adding are performed by:

a microprocessor,

a read-only memory including a program for processing the data, and

a random-access memory including registers suitable for recording variables modified during running of the program.

16. (Canceled)

17. (Currently Amended) An apparatus for processing a digital image, comprising means suitable for implementing the method according to claim 1 ~~any one of claims 1 and 4.~~

18. (Currently Amended) An apparatus for processing a digital image, comprising a device according to claim 8 ~~any one of claims 8 and 11~~.

19. (Previously Presented) A storage medium storing a computer-readable program for implementing a method for inserting according to Claim 1.

20. (Previously Presented) A storage medium according to Claim 19, wherein said storage medium is detachably mountable on a device for inserting a message that includes ordered symbols into digital data representative of physical quantities, and

wherein the device comprises:

means for segmenting the data into regions;

means for associating at least one region with each symbol to be inserted, said device further including:

means for determining a pseudo-random function, for each region into which a symbol in question is to be inserted, from a key which depends on an initial key and on a length of the message,

means for modulating the symbol in question by the previously determined pseudo-random function in order to supply a pseudo-random sequence, and

means for adding the pseudo-random sequence to the region in question,

wherein said means for determining a pseudo-random function is

configured in such a way that a dependence of the key on the length of the message is provided by a dependence of the key on:

the number of times the symbol to be inserted has already been inserted into other regions, and

the ranking of the symbol among the ordered symbols.

21. (Previously Presented) A storage medium according to Claim 19, wherein said storage medium is a floppy disk or a CD-ROM.

22. (Previously Presented) A computer program product embodying a computer program with executable instructions for causing a computer to perform a method of inserting according to Claim 1.

23. - 26. (Canceled)